技術戦略専門委員会グランドチャレンジ検討 WG
第３回会合議事要旨

１．日時　平成２０年１１月６日（木）１０：００～１２：３０

２．場所　内閣府本府５階特別会議室

３．出席者

［主　　査］
後藤 滋樹（早稲田大学教授）
［主査代理］
安達 淳　（国立情報学研究所）
［委　　員］
磯村 浩子（(社) 日本消費生活アドバイザー・コンサルタント協会）
伊藤 光恭（ＮＴＴ情報流通プラットフォーム研究所）
加藤 雅彦（(株) アイアイジェイ　テクノロジー　IBPS 本部）
楠　 正憲（マイクロソフト（株））
西本 逸郎（(株) ラック　サイバーリスク総合研究所）
二木 真明（住商情報システム（株））
松並 勝　（ソニーデジタルネットワークアプリケーションズ（株））
三河尻　浩泰　（(株) 富士通大分ラボラトリ）
森山 浩幹（(株) エヌ・ティ・ティ・ドコモ）
山田 安秀（(独) 情報処理推進機構）

（五十音順）

［政府］
内閣官房情報セキュリティセンター内閣参事官
内閣官房情報セキュリティセンター情報セキュリティ補佐官
内閣府政策統括官付参事官付
警察庁情報通信局情報技術解析課
総務省情報通信政策局情報通信政策課情報セキュリティ対策室
文部科学省大臣官房政策課情報化推進室
経済産業省商務情報政策局情報経済課情報セキュリティ政策室
防衛省運用企画局情報通信・研究課情報保証室

4．議事概要

＊＊
将来予測について（前回会合からの引き続き）
＊＊

○　SaaSという言葉は今流行であるが解釈の違が微妙にある。私自身はネット上に様々なサービスコンポーネントが配置されていて、例えば、ある会社の基幹システムを作る際に、それらをうまく束ねてフロントにユーザーインターフェースに当たるものを作れば、裏のコンポーネントは自由に選ぶことができ、自分たちに最適なものを選んで、通常なら何年かかかるような大きなシステムを非常に短期間で開発できるというものというようなイメージで捉えている。これは、いわゆる手作りのシステムからパッケージ化、半製品的なパッケージのカスタマイズという話だが、それでもビジネスのスピード感にシステムが追いつかず、もっと、早くするにはどうしたら良いかという流れの中で出てきた概念だと思っている。その中でクラウドなどにも関わるが、ネットワークベースでのサービスというものが、もっと一般的になってくるだろう。ただ、新しいセキュリティが出てくるかといえば難しいと思っていて、多くのものは、既存のブール系とかウェブサービスのセキュリティ対策の延長上にあるのかなと思っているが、一つ重要なポイントとなると思われるのは、ネットワーク上ではDoSとか、DDoSの対策が重要になると思う。

○　乱暴にいうと反論があるかもしれませんが、昔は一つのコンピューターの中でやっていたことが、社会的にも物理的にも広がり、大昔のプログラムといえばスクラッチから作る時代から、OSが出てきたり、APIが出てきたりして、自分の方では必要なことだけをすれば動くというような形になってきた。例えば、キャッシュというシステムもコンピューターの中でやることで、元々の意味は「隠しておく」という意味だったと思うが、そういうものが表に出てきた。一方で昔は広い範囲とか多くの部品を使っていたものが小さくなっているということで、興味深い。

○　電化製品のネットワーク化は相当に進んでいて、世界でも日本がかなりリードしていろいろなものを繋げてゆこうというようなことになっている。エコーネットあたりは、わざわざ線を引かずにいろいろなものを全て繋ごうという考えでいるようで、例えば、コンロとかそういうものも電化されて行くと繋がる要素になると思います。大前提として、いろいろなものがネットに繋がったときに何が起こるかということをセ

キュリティ面も含めて、今のうちに考えて行くことが、日本が先進的に世界に打ってゆけるという面から見て良いことだと思う。

○　家電については様々なところで検討があり、家電製品でカスタマイズされたものや、ユーザーの情報が入っているものを廃棄する際に、どこまで情報を消去するべきか、あるいはアップデート機能が付いているものでも、キーボードやディスプレイが必ずしも付いていないものが、アップデートに失敗した時の処理をどうするか、などの問題が取り上げられている。

○　家電の情報化に関する情報セキュリティ技術上の課題で追加したいが、Bluetooth が出現したときもホームネットワークが普及するのではないかと期待されたが、一つ課題になっているがペアリングだと思う。どのデバイス間の通信を許可するかを簡便に設定する方法は今でも無い状態である。PIN を入れることを考えてみても、キーボードがあるデバイスばかりではなく、利用者が簡便に特定のデバイス間の通信を許可する設定をして、かつ、それが理解できる方法というものは、セキュリティ上の課題で重要になってくると思う。

○　資料中の５年後の部分に書いたが、インターネットで VPN という使われ方が出てきて、今はクラウドコンピューティングということになって、ネットワークの向こう側にいろいろな計算機リソースがあって、それを使って行こうという流れが一つ出来ている。これがもう少し進むと特定の企業向けのクラウドの環境であるとか、特定のコンシューマー向けの環境などがネットワーク越しに作られて、ハードディスクをわざわざ販売店に買いに行くのではなくて、ネットワークの方で増設することで対応出来るようになる。そのために、今あるようなオープンなクラウドコンピューティングの環境に加えて、もう少し、A 社向けとか、B さん向けというクラウドなコンピューティング環境が出来て行くのではないか。

○　大規模環境ネットワークと書いているが、今はいろいろな研究が行われている。例えば、各装置の省電力化、センサーの進展、環境問題などを踏まえ、資源の有効利用、効率化、無駄な生産を抑制する需給調整等をすることを考えると、そのような情報を一極に集中して管理し、必要なところに必要なモノを送る様なことを、恐らく国家規模でなくては困ると思うがやってゆく必要があるのではないか。その際に、いろいろ

な個人情報も入るだろうし、有効に使うためには個人情報も必要かと思うが、そのようなところのセキュリティをうまく保ちつつ、大規模なネットワークとデータベースを管理する、データを上げる仕組みが必要ではないかと考えたもの。

○　いくつか、要素技術として挙げられているが、例えば「ライトウェイト認証」などのイメージだろうか。

○　まだ、具体的なところまで考えている訳ではないが、恐らく家庭であれば様々なセンサーが入ったときに、個人の情報を確保しつつセンターに送るような仕組みになると思う。すると、個人の情報も入るが、それを還元する方法も必要となるので、どのようにしたら良いかと思う。

○　今、環境省のプログラムなどでも、電力、特にエアコン制御、温度制御、適温のようなものも考慮すると言うことですが、電力会社の方に伺ったところ、地域ぐるみで取り組むと相当に効果があるとのことで、新しく開発されるような地域では、そういったことを考慮した町として設計することになっているようです。進めるのは大変結構なのですが、今言ったような考慮すべき点も充分あるのではないかと思います。

○　ここしばらく、グリッドでいろいろな複雑な計算をするということが進んできていると思うが、例えば、会社の中でもＰＣは高性能化しているが、実際にどのくらいＣＰＵリソースを使っているかと言えば、殆ど使われていないのが実情だと思う。そこで、今のグリッドの延長上に何があるのかを考えると、物理サーバーの上に仮想の環境を作って、そこで、仮想ＰＣとか仮想サーバーをつくるということができないかと常々思っている。もし、このようなことができれば、大きなパラダイムシフトになる。そして、恐らく、グリッド全体を管理するベースとなる機構というものは、今でいうP2P 的な動きになってくる。今、P2P のネットワークで問題になっているのは、これをうまく制御できず野放しになってしまうことで、万一マルウェアに感染したときには、モグラたたきになってしまうとか、そういう問題が恐らく出てくると思う。P2P というものは、この winny 騒ぎのおかげでイメージが悪くなってしまっているが、技術としては面白いと思っており、これをうまく制御できるような技術を確立して行くという様なことも含めて必要ではないかと思う。

○　確かにP2Pだと制御しにくく見えない。先程委員が言っていたVPNなども、最近のアナライザーなどは、キーを入れるとVPNでもIPsecが見えるものも販売されている様だが、一般には一瞬は見えないという形になっている。あるいは、光の中を束になって通っているという状況になると、なおさら管理する側から見えないということになる。将来ネットワークというものはいろいろな像があるが、今のＩＰパケットがバラバラと行くところが見るという意味では、見やすいと言うことになっている。どこまで見えるようにしなければならないか、見えすぎると通信の秘密であるとか、プライバシーとか、いろいろ、問題も増えてくるような気もする。

○　出てきたキーワードを見て行くと、ＶＰＮ、クラウド、SaaS、SOAI、P2P、グリッドなどで、恐らく全体の情報処理のテクノロジーの流れというのは、仮想化が進んで行く方向にある。実態はどこにあるのか分からないが、ファンクションがどこかに見えていて、それをいろいろなレイヤーで集めてきて、例えば、ネットワークのレイヤーが潰れるとオーバーレイになるし、サービスのレイヤーが潰れるとSaaSとなるような形で捉えていって良いだろうか。

○　方向としては、そうではないか。オーバーレイなどは次世代といわれるものを見ていると、もちろん物理限界はあるもののルーターなども仮想化するという、文字通りのオーバーレイ、実態がどこにあるのか分からない時代になってくるという方向ではあるようだ。

○　情報セキュリティの対策では、孫子の兵法にもあるように敵を知り己を知れば百戦危うからずと言いながら、敵をわれわれは知りにくい。先ほど話があったように、実態がどこにあるか分からないような状態がますます進んで行く方向にあるのは間違いので、敵をきちんと知らなくてはならない。これは、予測を実現するために必要とされる技術（２）に書いてあることだが、そのベースとなる敵を知ることだけでなくて、世の中全体世界の情報セキュリティ政策とか、情報セキュリティ産業の構造がどのようになっているかなどをしっかりと把握することが重要なのではないか。これは、文部科学省の情報爆発のプロジェクトにも出ていることなので、テクニカルな要素技術は既に詰められているのではないかと思うが、それを活用しつつ行えば良い。そのケーススタディとして(2)を挙げたが、特に、アングラの情報をどうやって収集するのか、表に出ている情報セキュリティだけでなく、アングラの情報をつかむと言うことが重

要。最近よく言われている標的型攻撃は、個別の企業、組織に対して直接不審なメールが送られて情報が摂取されるものだが、攻撃する側は攻撃対象の状況をよく把握しているが、攻撃される側は個別の企業や組織の間で情報が共有されずに、分断されているので把握できていないという、経済学でいうところの「囚人のジレンマ」みたいなことが生じている。世界全体として不利益が生じていて、対策が講じられないという状況があるので、それに対して、日本全体としてきちんと対応して行く必要があるのではないか。

○　最近感じることだが、攻撃情報の収集といっても、今我々がやっているのは飛んでくるミサイルを着弾するまでの間に分析しているというのが現実だと思う。どこに発射基地があって、だれがそれをコントロールしていて、どういう組織がそこに関与しているかということを知らないで攻撃情報の収集と言っても、これは全く不均衡で守る側からすれば、とんでもないことなわけだが、これを日本で推進して行くことは非常に難しいことだと思う。ただ、もし我々が世界をリードしてそういったことをしっかりと出来ると言うことになれば非常にポイントとなろうかと思うので、観点としては、飛んでくるミサイルだけではなくて、その背後にある実態をつかんで行くと言うことがキーになると思いますし、それができないと無理だと思う。今日本を標的としている攻撃の大部分は日本国外からのものだろうと推測されるが、攻撃者は自分が捕まるという認識を持っているとは到底思えない、とても馬鹿にされた状況でやられてしまっているので、このようなことは我々民間レベルでは対策も非常に限られているので、是非、国を挙げてやって欲しいと思う。

○　(P. 18 について)書いてあるもので理解頂けると思います。

○　様々なものが、パッチを当てるようになるとの話しは既にあったが、HD レコーダーのバージョンアップが電波によって自動的に行われて、バージョンアップ後に操作方法が変わったことによる誤操作が問題となることがあったり、ユーザーのどれほどが認識しているかは別として、一部の機器の脆弱性情報が公開されている問題がある。一方で、携帯電話のようなものは相変わらす基本部分はユーザーには変えられないようになっており、何か問題が起こったときには一旦預ける形となって、大変なコストがかかっているという話しも聞く。これを避けるのは、委員が書かれているようにいろんなところに問題としては関係があります。

○　技術としては階層があって、一番上には正しいソフトウェアを仕様どおり早く作るという技術があり、一番下にはパッチのディストリビューションの方法、データリンクのところまで降りて行くというプリミティブなものの間の中で、異なるコンフィギュレーションに対して正しいパッチを自動的に生成するような技術というのは、恐らく技術の階層があるのだと思うのですが、このあたりはどうだろうか。

○　パッチで非常に難しいのは開発のコストではなく（開発は、場所を見つければ何行か書き換えるだけなので)、むしろ、様々な構成にそのパッチを当てたときに問題が起こらないか確認するというテスティングコストの問題だと思う。また、配布がこれまで再起動を伴うことが多かったのは、モジュールが再起動されることを前提としていない構成となっている場合が非常に多かったことによるものだが、５年くらい前から徐々に動作させながらパッチを適用できるようにソフトウェアの仕様そのものを変えるという作業を地道にやっており改善されてきている。恐らくＣ言語で書いている限り vulnerability が無くなることは無いだろうが､特に古いソフトの資産のことを考えると、いくら関数型言語が素晴らしいからといっても、それでＯＳを書くというのは現実的ではないだろう。

特にパソコンの世界で出来ていて、家電の世界で出来ていないのは、バージョン管理ではないかと思う。私どものＯＳで言えば４年に一度分岐するが、それ以外はそれほど分岐していない。ところが、家電については恐らく春秋の年に２回くらいバージョンが分岐されていて、ソフトウェアの構成管理という点で苦労されているのではないかと想像している。携帯で動きが進んでいるが、ＯＳの標準化とかバージョンの切り替わりのタームを長くしてゆくなど、ベタな対応というのは今後進んで行くのではないか。

○　これは、セキュリティパッチという領域の話しではなくて、ソフトウェアのメンテナンスも含めた作り方に関する系統的な方法だ。

○　売るまでよりも、売ってからの方が費用がかかるようになっているのに、特に家電等のハードウェアについては、収益が発生しないモデルから抜け切れていない。ここは非常に大変だろう。

○　Ｐ１９は前回議論しましたので、もう一度見て頂ければと思います。

○　これはプログラムだけを見ているが、他にも例えばインターネットにしても、全ての人が自分の端末に他の全ての人の端末が接続されている必要というのは無いと思う。ごく限られたアクティビティだけあれば足りるのではないか。人々の日々の活動が区分けされているとして、その区分けされている区間でアクティブな領域をセキュアにする。それは、ここに書かれているアプリケーションも含めた状態で実現されるべきで、例えばネットワークで言えば、お母さんのＶＰＮとか、お父さんが仕事で使うＶＰＮとか、お父さんがエンターテイメントで使うＶＰＮとか、そのような形で捉えてよいのだろうか。

○　ＷＥＢとかメールくらいしか使わないというのと同じように、通信する相手というのが時間帯で決まってくると、仕事とプライベートを分けることもできる。

○　使っている人、タスク、性質などによる。ＷＥＢもバンキングしている時と、単にサーフィングしているときとでは状況が違ってくる。

○　書いた以外には、いわゆる仮想化やクラウドの話しになると実態がどうなっているか分からないということがある。我々がサイバー空間の中で扱うものは情報しかないが、その情報は現在のところ比較的物理的なデバイスに近いところにあって問題となっていないが、仮想化が進展して行くと箱と情報というものの紐が弱くなって行くと考えられる。すると、セキュリティの観点からはインテグリティが重要になってくる。そのデータは本物ですか？それは、本当に私のデータですか？と。また、情報というのは意識的に気を付けていないと次々に蒸発してゆくと最近感じていて、例えば古いコンピューターの情報を記録したフロッピーディスクは、最近のパソコンでは読むことが出来なくなっている。それが、このまま進むと資料に書いたことが起きると考える。

○　スペクトラムとしては結構広いと思うが、必要とされる要素技術をみると、実態が全くない電子マネーが一番良い例だと思うが、単なるビット列が唯一無二の本物であるかどうかを保障する技術というものが注目されてくるという風に捉えて良いか。

○　ＤＲＭと書いたが、ＤＲＭと書くと何となく誤解されるような気がするので、現状のＤＲＭとは異なると書いた。

○　最近は電子マネーがマネーロンダリングに使われているという問題がクローズアップされている。これは技術で解決できると思っている。そのあたりにも、絡んでくるだろう。

○　ＤＲＭという言葉に絡んでですが、今の音楽ＤＲＭに限らずビット列がサーバー上の鍵と紐づけられていて、ビット列単体では機能しないようなソフトウェアが増えている。一方で事業の継続性という点では疑わしい部分もたくさんあり、先日もウォルマートがＤＲＭサーバーを止めるといって、これまで買った楽曲をどうするのだという議論があった。本来情報を守るための技術によって、情報が失われてしまうリスクをどう考えるのか。それを民間企業の経営の継続性だけで考えてしまうと逆に新規事業者というのは参入が難しい、あるいは、同じことをやろうとしても消費者から受け入れられないことになるので、如何にデータが人為的に蒸発しないようにするかということが論点になると思います。

○　携帯電話でもそうだと思う。自分でダウンロードした楽曲でも、携帯を買い換えると新しいものに移せない。そこへ入れると二度と取り出せなる。自分で取った写真が、メールでも取り出せなくなってしまう。自分で撮った写真が送れないというのは、どういうことなのか。

○　私の家族も携帯が故障して、保証によって全く同じ機種がもらえたのですが、古いものから新しいものに情報を移すことについては、お店の人と２時間くらい格闘したと聞いている。自分のデータなのにも関わらず。ですから、守るということの他にエスクローの技術とか、いざとなったら、この人に頼めばレスキューしてもらえるという道というのも社会全体としては必要ではないか。大きな意味でのインテグリティとか、セキュリティとか信頼感という意味では、そういったことも必要。

○　自分のデータなのに自分が自由に出来ないという状況というのは、今は非常に多いと思う。音楽をダウンロードするのに何百円払いましたが、携帯が壊れたら全部無くなりました、同じものをダウンロードするなら、また、お金を払ってくださいとなると、２回目のお金は何のために払っているのかということが明確ではない。

○　利用許諾を良く読むと、下のところに小さな文字で書いてあるのだろう。
その当たりを解決するのが、次の伊藤委員のご意見ではないですか。

○　携帯やスマートフォンも含めて、写真を撮って友人に送ろうとか、会議のレポートをするときなどに、文章だけでなくて写真や動画を送るということがこれから進んで行くと思います。そう思ったときに、最初送った時には A,B,C の３人に送ったけれども、翌日になったら他の人にも送りたいということも結構あると思いますが、いちいち送るというのは結構面倒で携帯端末なりスマートフォンの方にもっと大きなストレージがあって、そちらの方に自分のデータを入れて、URL になるかどうかは分かりませんが、アクセス先を連絡することによって、そこを見てもらうという利用形態がこれから進んで行くのではないかということが P21 のポイントです。また、もう一つのポイントが､アクセス先をオープンにしたときに､特定の人だけに見て欲しいときに、パスワードとかではなくて、もっと簡便に、例えば SIM カードなどを使用した認証をしてゆくなどの方法がセキュリティを向上させる手段になって行くのではないかと思います。

○　携帯電話には中に何か入っているイメージがありますが、私の持っているイメージはそうではなくて、携帯電話は単なるアクセスデバイスであって、携帯の網が提供する便利なサービスも含めた単なる入口にすぎない。認証は何か別のメカニズムでそれと紐づけられていて、実際すべのサービスは網上にある、というものだと思う。今でも電話帳はネット上で「お預かりサービス」というのがありますが、あのイメージ。データは網上にあって携帯電話はキャッシュが入っているだけ。もし、壊れてもパット捨てて、その辺にあるキオスクなどで新しいものを買うスタイル。

○　ネットワーク上にストレージがあって、そこを知せると言うことですね。

○　弊社は今そちらに向かっていて、完全に端末側のコピーというのは、クラウドのキャッシュであるという考え方で、どこまでどうキャッシュするかというのを端末の capability に応じてコントロールをして行こうとしています。なおかつ、全てクラウドにあるということは、誰がそれにアクセスして良いかと言うことをシェアして行けば、端末側でアンマネージなコピーを増やさないで、その人たちに必要な情報が行き渡るような仕組みも出来ますので、その中で、例えばビデオをどこまで見たというような情報をメタデータとして持っておけば、例えば、家を出るまでテレビで見ていたビデオを､家を出てからは携帯で続きを見られるということも簡単にできますし､徐々に端末というのは、クラウドのキャッシュに近くなって行くのではないかと思っている。

○　最近 PC のシンクライアント化というのが流行ですが、携帯端末のシンクライアント化というイメージなのかなと思います。先程､「電話帳お預かりサービス」というお話しがありましたが、私の会社では標準で導入しています。しかし、現場からは使い勝手が悪いという評価です。何が使えないかというと、まず、重い、それから、着信電話番号に対応する電話帳データが端末に無いので、誰から掛かってきたか表示されないという点にあります。ただ、そういった問題が解決できれば、今の様なお話しは進むのではないかと思います。今は、WEB ベースでやっていますが、それをちょっとしたアプリケーションでリアルタイムの通信をしながら、ローカルの電話帳と同じような動きが出来るようになれば、より普及して行くのかなという気がしています。

○　今の話しを実現するためには、クラウドにＷＥＢ経由でしかアクセスできないというのはダメで、端末側にもう少しインテリジェンスが必要になってくると思います。このあたりは、グーグルが Android などで取り組んでおり、マイクロソフトでも Windows Mobile では電話帳をクラウドから導出する訳ですが、当然、端末側の使い勝手としては端末に登録されている電話帳と同じようなユーザーエクスペリエンスであることが期待されるので、そこをいかにシームレスにしてゆけるかということが非常に重要だと思います。一方で、そこをシームレスにすることによるセキュリティ上の問題というものもたくさん出てくると思います。例えば、自分の電話帳に登録している全員にスパムを送るというウィルスに感染してしまう場合も出てくるので、そこのセキュリティをどうして行くのかと言うことが非常に重要な問題になると思います。

○　ご存じのとおり、日本では振り込め詐欺が非常に流行っているが、韓国ではボイス

フィッシィングと言われているらしく、韓国では外国からの振込詐欺などが電話経由で掛かってくるそうです。ですから先程の話は間違いなく、そういった犯罪のプラットフォームになるでしょうし、さらにＩＰになると全てがクラウドの中へ置かれ、そのプラグが携帯電話だったり、PC だったりすることになり、そのプラグを経由してしか行為者のことが把握できないようになる。そこで、リテラシーの問題とともに、そういったことを許さない機構というのを如何に設置するかとういうことも忘れてはならないと思います。

○　先程の途中で仕事を止めて、続けるというのは Unix になってからは、プロセスは端末から起動されるので、端末が切れると終了して残っているとゾンビなどと言われますが、昔の ARPANET で使われた TENEX という OS を商用化した DEC の SYSTEM20 というものでは、detach, attach というコマンドで一度 detach して、また、attach するということを頻繁に使っていました、UNIX でもそれをシュミレートしたソフトがありまして、私もしばらく使っていました。文来、途中で止めて再開するということは、やればできるというものであるとは思いますが。

○　その手の技術は、今、仮想化の専門家が非常に研究をしています。クラウドの中において１台で行っていた仕事を２台に分けることや、ライブマイクレーションと言うのですが、ダイナミックにリソースを振り分けている時に、OS のインスタンス毎 0.1 秒とか、ミリセック単位のラグで１台で動いていたのを２台にするなど、今のプロセス構造体ではやりにくいところもあるのですが、仮想化においてそういった技術が再び脚光を浴びています。

○　議論は、既にサービスというところに入ってきておりますが、一つ一つと言うことだと時間もありませんので、ここから先は、それぞれ強調されたいところとか、他の方から質問があるというようなところがあれば、お願いします。

○　自ら言っているのですが、ＬＴＥとか高速になるほど携帯に入っている情報というのは、センター管理されてゆく方向にはあると思っています。電話帳などは最たるものだと思うし、先程からの議論についてもそのとおりだと思っている。ただ、当社もそういったことについてはロック機能であるとか、既に実施している電話帳お預かりというサービスでは、携帯の中に入っているものと同期を取っている。そういうもう

少し手前のところの、ロックであるとかセキュリティを守る技術というのは、今でもやっている状況です。センター側のアドレス帳の問題も、私もあるところでその議論はしているのですが、私たちがサービスしているのは番号案内サービスではなくて、番号を通知するサービスであって、アドレス帳に変換しているのは携帯の中での事なので、ネットワークやプロトコルをかなり考えないと、なかなか出来ないことかなと思います。そうなってくると、センター側で管理したもののセキュリティを守ることが必要なのですが、そこの間にあるのが、如何にセキュリティを保ちながら簡便にアクセスをするかという問題だと思っています。私たちがいつも戦っているのはそこの部分で、先程から知的財産の話しなどがあるように、私たちが新しいサービスを出すときに、１／３位は法務担当と話しをしますから、規約類もそのたびに一生懸命書いて直す作業を繰り返さないと出来ないとか、権利の問題も含めて私たちがやりたくても出来ないことというのは非常にたくさんあります。少し外れますが、携帯などは良い例として、私どもが出した携帯はある程度まで私どもの方で守っているところがあります。いろんなインターフェースは、これ以上は触らせない、例えばＧＰＳを触らせるのはアプリにしても限られた許可されたものに限るなどのことがあります。コマンドもいろいろあるが、触れるもの触れないもの、著作権上ここはダメだというものは皆制限している。問題は、これから Windows Mobile や Android が入ってきたときに、そういう問題がどうなるかということ。極端な例では、自動車の様な世界も自動車のネットワーク化を進めるときに、カバーしている部分がある。自動車のメーカーがこれ以上は出さないと守っているところがある。今､携帯の中で起きていることは、恐らく、そこを守っているのだが、オープン化という議論の中からそこが解放されて行くと、セキュリティの問題が発生するのではないかということ。そこは、家電製品全般に言えると思う。オープン化を進めなければならないという議論もあるとは思うが、そこは、これからセキュリティを論じる上で、ベンダーとかメーカーが守っているところと、オープン化という、そこを独占してはいけないという部分の間で、セキュリティをどう守って行くかは技術的にはうまく言えないのですが、大きな問題かなと思っています。

○　まさにそこは通信プラットフォーム研究会で議論されていたところだと思うのですが、２つ必要だと思っており、垂直統合・マネージドで誰でも安心して使えるという世界と、自己責任・アラカルトで自由に使えるという世界と両方やって行かざるを得ない。水平分業と垂直統合というのが両方無くてはならないし、そこで、自己責任の世界というのは、こういう大変なところもあるのだというところをしっかり消費者に伝えていかないとミスリーディングとなる。その辺で iPhone などは非常に苦労しているところがあると思うが、かといって垂直統合だけの世界ではイノベーションが止

まったり、新しいアイデアがマーケットに出ていかないことになるので、そこは両方を出来るようにすべきというのと、その中で、消費者がだまし討ちに会わないための仕組みを造って行くことが重要であると思います。

○　誰がどこをやってくれるのか､あるいは､やらなくてはいけないのかということを、社会全体としても見直して行く必要がある。課題は大きいわけですが、その殆どのところに、セキュリティの話しが絡んでいるというのは事実だと思います。

○　今、森山委員が言っていたオープン化ということがキーワードだと思っています。それは、携帯ですとか家電だけではなく、日本が一番強みを持っている自動車でもそういったことが起きている。今、自動車の IT 利用はカーナビなど情報提供や警報目的なものが中心ですが、これが、いずれは ECU（エンジン・コントロール・ユニット）など車体の制御の方に繋がって行くわけです。今はどのメーカーも、上の方から下を制御することにならないようにしています。例えば、制御の状態がディスプレイに表示される方向、つまり下から上への方向はありますが、反対に上から下に情報が行く形になるとと､誰かに情報が乗っ取られた場合に自動車がおかしな運転をされて、人命に関わることになるおそれがあります。今はそう出来ないようになっています。しかし、いずれは自動車の ITS 化の進歩に従って、上から下へという情報の流通も出てくると思います。それに対応するセキュリティ技術をきちんとやる必要があると思っています。また､セキュリティ事故の責任が運転者にあるのか､ITS 側にあるのか、もっと別のところにあるのかをログとして記録する、いわゆる「ドライブシュミレーター」が必要になるでしょう。これらは複数省庁に跨った事項なので、NISC のリーダーシップの下でやるという意味においては相応しいかなと思っています。今、社会制度の現状ですと、もし、事故があったときには全部運転者の責任になってしまっていますが、その制度自体も大きく変革させなければならないということもあり、社会の変革を先取りしながら、あるいは、変革をさせるようにして行くという、制度設計ということも含めてやって行く必要があるグランドチャレンジテーマではないか。

○　今の社会インフラ的なシステム・サービスの話しですが、交通システムで常々思うのは電車がよく遅れること。私は京浜東北線で通勤してますが、大宮辺りで事故が起きると、横浜まで止まることがある。というのも、朝の時間は殆ど見える位の距離、間隔で電車が走っていて、どうにもならなくなるらしいのです。今は、ＡＴＣ（自動列車制御装置）などで制御をして、ギリギリの間隔で詰めて走らせている。それ故に

何かひとつ問題が起きると、全体に非常に大きな影響が及ぶ。自動車なども将来的には、例えば高速道路に上がったら後はハンドルから手を離しても目的地までは自動的にコントロールされるという話となり効率よく行くようになると思うが、万一、制御システム全体に問題が起きたようなケースが発生した場合に、どのようにリカバリーするのかということも含め、きちんとシステムとして考えて行く、もしくは、そういう場合に端末にあたる自動車や電車がどういう挙動をとるのかという事も含めて、全体を考えて行く必要があるのではないかと思う。あまりにも効率を追いかけすぎると、何か起こったときに大きなカタルシスになってしまうおそれがある。

○　恐らく自動操縦という点では、飛行機が一番進んでいると思うが、機械に出来ることは、フライ・バイ・ワイヤ（電気的な操縦・飛行制御システム）が切れたときに、ラダーの向きがフェイルセーフで、一番飛行機が安定する姿勢となるように設計するとか、自動制御出来なくなったときに手動に切り替えるというところまでだと思う。一方で、危機管理が出来ているのかという話しで思い出しましたが、阪神大震災の後に、スーパーマーケットで非常に困ったのが発注管理が出来なくなったということ、つまり、みんなＰＯＳに慣れきってしまって、何をいくつ発注して良いか頭で考えることが出来なくなっていたという話しがありました。手動に切り替えたときに人が対応できるのかという点について、自動化が進むに従って人間社会の方でそういったノウハウが失われて行くということが非常に深刻な問題だと思います。このように、機械にできることが自動でうまく行かなかったときの対応策が手動に切り替えることだとした場合に、如何に手動に切り替わったときに人が適応できる能力を残してゆくかは重要な課題だと思います。

○　それは、パーソナルなインプレですが、グランドチャレンジだと思う。

○　それはそうです。もう、このごろ割り算というのは暗算で出来ないですし、子どものころは平方根の計算も紙があればできたような気がするのですが、今はやる必要もなくなっている。漢字なども書けなくなってきて、時々授業中に学生に聞くと、学生も分からなくて電子辞書を引いて…ということもあります。全部パワーポイントになっていると、先生も書かない、学生もプリントするだけなので書かない。ですから、人間というのは新しいことが出来るようになっているが、前に出来たことが出来なくなっているというのは、個体別でもそうです。

○　今の手動に切り替えるというのは、もう少し一般的に考えると先程の話しだとクラウドのように情報はどこかへ行って、手元はそれを操作するロジックだけという形になるとディザスターが起こったときにどうするか。例えば、電話番号も分からないとか、そんな状況になるのに対して何を補償するか、別の方法、そんなフェイルセーフのようなシステムを組んでおく必要がある。そういう方法を考えなくてはならないと思う。また、先程の交通システムの話しですが、鉄道などは closed なマネージをされて提供するサービスに対して何らかの保障をしている。それに対して自動車のようなシステムは、自由度が大きくどこにでも行けるが、その代わり事故が起こったときには自分の責任と言うことになっている。それが、情報システムを使ってコントロールされて行くと、たとえば、そのような状況で交通事故が起こったときには誰の責任なのか、運転していた人の責任ではなくて情報システムの責任でしょうということになると、鉄道のようなことになって、あなたが享受できるサービスは、ここまでですよと。失うもの、ケータイに入っている写真が外では使えないというのと全く同じ様な形で、あるサービスとしてクローズドなシステムを作ってやっている。それをオープンにすると、それに対して、会社とかが負わなくてはならない責任が大きくなっていって、非常にコストの高いものになる。そこで、うまいバランスを見つけなければならない話しなのかなと思いました。

○　社会全体としてどう変わって行くのかということですが、そこで選択の余地があるのならば、選択の余地があると納得した上でやった進めた方が本当は良い。何となくそうなってしまったと言うことでは、なかなか納得できない。

○　PL 法との関係もある。要は製造物責任という部分を突き詰めて行くと、誰もモノを造らなくなる。あまりにアレルギー体質になっている部分がある。もちろん、製造物の責任というのは当然問うてゆかなくてはならないが、それに依存しきって盲目的に信じてしまってはいけないとう部分もあるので、そのあたり、利用者の責任という部分は、どこかでしっかりと問わなくてはならないと私は思う。

○　確かに、子どもの時にどういったことを心得なければならないかという話しにも繋がるが、教育というものは年数が掛かるものなので、その間に世の中の方が変わってしまう状況ですので難しいところ。

○　製造物責任は、ウィルスの大規模感染があったときに大分調べたのですが、モノに対する責任となっている。ところが、セキュリティで今問題になっているのは、まさに、クラウド上の様々なサービスと連携しながらモノがインテリジェントになってゆく世界の中で､そこの連携対象というのは日本法の外側にある場合も結構ある訳です。仮にアメリカのクラウドに存在するあるメタデータを参考にした自動車が日本国内で事故を起こしてしまった場合に、今は日本の自動車メーカーに対しては責任を問えるけれども、それが見に行った誤ったデータをフィードしているところまで責任を問うことは非常に難しい。恐らく２，３考えなくてはならないと思うが、一つは先ほど電車の連絡の話しもありましたが、今後起こってくる事故の多くが単一の製造者ではなくて、非常に複雑な事業者間の関係の中で問題が起こって行くこと。それに対して適切に原因を把握して、合理的な判断をして行かなくてはならない。さりながら、そういうインテリジェンスが社会から求められるということは、全体としてみれば事故は減ると思うのです。つまり、自動運転機能で車庫入れをして、何万回に一回は失敗するかもしれないが、下手な人も上手い人もいる人間がやるよりは、割合としては低くなるはずなので、逆に言えば社会的コストを誰がどう負担するかのルールさえ明確になっていれば、社会が負担可能なコストではないかと思う。最後に、何がどうおこるかということを事前に予期しにくい世界になってきた時に、司法の役割がますます重要になってくると思うが、日本では裁判沙汰という言葉もあるように、出るところへ出ると言うことを極力回避しようとするところがありますし、行政のスタイルも、事前に出来るだけ考えるということがありますので、将来を予期しにくい社会で、如何に低い行政コストで安全性と公正さを担保して行くかということについてのグランドデザインというものは必要になってくると思います。

○　事前型と事後型というのは、もう一つの議論のテーマであるプロジェクト管理の進め方などに関係がある。従来型というのは、公のプロジェクトは事前にかなり考えてあるので、途中で変えにくいというような指摘があった。少し議論もしたが、指摘のとおり世の中の仕組み全体というところが大きく関わるのかなと、しかし、かなりの範囲で納得してもらってやらないと､なかなか社会全体としてうまく行かないだろう。

○　先日、製造業の方から話しを聞く機会があり、彼らが一番悩んでいることとは、多品種少量生産になっていて、如何に期間を短縮して世の中に出して行くかを考えている問題であると。それで、その会社が何をやっているかというと、検査工程とか品質管理工程というものを割愛していて、また、最後に良いものだけ弾いて、（今までは悪いものを弾く）世の中に出すなど、いろいろなことを考えていると聞きました。

その中でヒントになるかなと思ったのは、みなで議論していると品質を弱めるツボのようなものがあって、それを出し合い、そこだけチェックをして全面的な検査を止めることによって、かなり成功していると聞いています。よって、セキュリティを守るときでもコツを考えるというか、全てを検査とか試験の対象としてセキュリティを守りすぎてしまうと、恐らく、コストに跳ね上がって、結局先ほどの話しにもあったとおりモノを造らない文化も産まれてしまうかもしれないので、その辺りをうまく、アーキテクチャーなのか何なのか分かりませんけれど、ここと、ここを守ればという議論が出来れば面白いかなと思いました。

○　世の中の変化でどうなって行くか分からないが、ここから先の経済情勢で日本の果たす役割が従来とかなり分担が変わってきたときに、よく言う、ガラパゴスは素敵なのだけれど高いということで、安いものをドンドン造るということを日本がやるようになったら、日本の世の中の仕組みもそのように割り切る部分が出てきて変わってゆくのかなという感じもする。従来の日本型はしっかり造るということにあり、例えば、半導体が出始めた時代は、店頭で販売する時点でも不良品が多かったが、日本の半導体が殆ど 100%のイールド率を誇っているのに、さらに全数検査して出荷するということになり、日本製の半導体のテスターが世界を席巻したということもありました。ですから、充分時間を掛けると日本が出てくるというのがありますが、最初は歩留まりが悪くても先に出す方が市場を押さえてしまうということがあるかもしれない。

○　宿題のペーパーを見るとプライバシーという言葉があちこちに出ていて、技術的に出来ることは非常に増えている。例えばカーナビだが、自動車のバンパーにカメラを付けて、その映像を１週間くらいカーナビに保管をしておき、事故が起こったときに、その時の映像を引き出すということが技術的には可能だが、それは果たして道義上やってよいか、また、ストリートビューなどは問題になっているが、カメラメーカーから GPS デジカメが発売されて、これから多くの写真に正確な時刻と位置が入ってくるようになる。これがクラウド上にアップロードされて公開されときには、いつ、誰が、どこにいたというメタデーターが簡単に張り付いてしまっているということが３年から５年で起こってくる。このようなとき、これまでの日本におけるプライバシー法規を巡る議論というのは、住基ネットで国民総背番号が良いかというような、非常に単線的で４情報（氏名、住所、性別、生年月日）をどうやって守るかというような話しだけだったが、むしろ被写体のプライバシーとかクラウド上に浮かんでいる個人の行動履歴に対するメタデーターとか、特にそれが個人情報と紐付いていない ID でしかない情報の場合のプライバシーの議論というのは、ほとんど行われていないよう

な現状があると思う。ヨーロッパなどではＥコマース指令などから手を付け始めているところだと思うが、そこは、多分社会的合意を造って行く必要が向こう５年から１０年にかけてあると思いますし、同時にそういった社会的合意に基づいて利活用とプライバシーを両立させて行くための暗号の応用に近い技術開発が活発に進のではないかと考えている。

○　確かに、従来のプライバシーに関する社会全体の議論は、必ずしも日本では成功してこなかったし、まだ、多くの課題が残っていると思う。

○　個々のデータに何が写っているのかということは、比較的守りやすいと思うが、それを網羅的に演算して、新しいデータを何か作り出すという行為というものを技術的に禁止するというのは、なかなか難しいと思う。

○　たしか、オーストリアの電子政府か何かでは、アプリケーション毎に違う ID を発行して、その ID を紐づける行為に対して刑事罰を科してしている例があったと思います。

○　しかし、出来ることは出来てしまう。

○　そこは難しくて、技術的に強制する方法としては、例えば、アプリケーション毎に違う ID を使うとか、それをアプリケーション ID と個人 ID を紐づけてハッシュオフするとか、いろいろなやり方があると思いますし、恐らく法的な強制に関する議論というものも、本当にそれが、すべきものがあれば考えられると思います。

話は変わりますが、考えなくてはいけないもとして、今でも画像検索で自分の名前を入れると自分の顔が出てきますが、全てのネット上にアップされている自分の顔とその名前が紐付いたときに、自分が写っている世界中のクラウド上の写真がばっと検索結果で出てきて、何時どこで撮った写真ということがわかれば、何時、何処にいたかということが分かることになる。多分これは、困る人が結構沢山いると思いますが、そのようなことは、今の法制度の中では多分考えられていないと思う。既に、何時何処で食事したということを、食べた相手にブログに書かれて、どこかでついた嘘がばれたということは結構起こっていると思うのですが、その辺はこれから５年くらいで

ますます、考えなくてはならないと思います。

○　情報セキュリティ基本計画などでも書こうとしているとおり、エンドユーザー、会社の経営者、ディベロッパーそれぞれの立場での情報セキュリティに関する相場感の様なものが今後、しっかりと出てこなくてはいけなくて、そのための社会的な取り組みというものもあるだろう。また、相場観が出来上がったときに、それを技術的に強制するためのメカニズムが必要で、この２つを併記しないとダメだ。その相場観が出来上がったときに、それを保障するための要素技術をいくつか並べて行くのことになるのだろう。ただ、これを一緒にするとは言っても、法制度がねという人が出てくる。

○　今の話しに関連させていただきたいと思うのですが、脆弱性の届け出というものがあり、今まではソフトウェア製品ですとか、ウェブアプリの脆弱性の届け出が殆どだったのですが、全体の中では少ないですが組み込みソフト製品の脆弱性の届け出もあります。これは、ハードウェアに組み込まれたものなのでＰＬに関係しかねない。しかし、先ほど委員から指摘がありましたように、今の届け出の内容は、人命とか人の健康に関係するものは無いですけれど、将来そういうことがあるかもしれない。それをギリギリ詰めて行くとディベロッパーの開発意欲をそぐことになり、また、利用者の選択の責任をどうするかという問題もある。そうすると、選択をするといっても、利用者が、消費者あるいは経済人として選択する判断をするための適切な情報が、ディベロッパーなどから与えられているかというと、ほとんど無い状態がある。仮に与えられていても、利用者が理解できるか、また理解できる分かりやすい情報が与えられているか、という問題もある。従って、利用者が適切に判断できるセキュリティも含めた諸元というものを、法制度で縛る前のワンクッション置いた中間的な形での、ガイドライン的なものが必要ではないか。これによって消費者の目も肥えるということに繋がるわけで、そういうことを我々IPA として議論し始めている。このようなことは、全体のレベルを上げる一つのステップかもしれないと思っている。

○　今、利用者とか消費者の問題が出ましたが、この世界において一般の消費者として知ることができる情報や知識は非常に少ないと思う。個別の電化製品などで現在のＰＬ法でも対象になるようなもので損害などが起きた場合についても、今の表示の問題とかそれを理解できる能力などの点で、非常にこの分野というのは遅れている状況にあると思う。先ほど法律に無い場合の諸元という話がありましたが、そこで一般消費者に対する広報とか、教育とか、リスクコミュニケーションとかの機会をもっと増や

す必要があると思う。今は、この世界の催し物に参加してみても殆ど消費者の姿がなく場違いな感じがします。もう少し基本的なレベルで、一般の者にもこのようなリスクがあるということが分かるような状況にして行く必要があると思います。

○　基本計画検討委員会において、先ほど委員から話のあった組込ソフトの話と同様にE-コマースにおける損害の責任をどうするのかという議論が出ております。オークションサイトのＩＤが盗まれて発生した損害をどうするのかという観点で、消費者に対する説明責任や、どこまでを会社側が、どこまでを消費者側が、責任として負うのかということが議論されました。先ほどの話と同じように、いきなり法律というのは難しいので、ガイドラインか、リーディングカンパニーのようなところが率先して何か説明をするなど、そういう方式はとれないのかという話しをしていたところです。

○　先ほど発言のあったリスクコミュニケーションについて、技術的な開発の切り口もあると思う。ベンダーとユーザーとのリスクコミュニケーションというのは、今は、約款か何かの小さな文字に書いてあるところで全て行われているが、保険などについて考えると、一般的なものであれば何となく相場観があるので、そんなに詳しく読まなくても、さほど酷いことが書いてあるとは思わない。ただ、特別に作ってもらったようなサービスであれば、とんでもないことが書いてあるかもしれないので、文字に依存しないリスクコミュニケーションの方法というのがあった方が良いと思う。

○　なかなかエンドユーザー・ライセンス・アグリーメント（使用許諾契約書）は読まれないのですが、あれは結局のところ法的責任範囲を明確化するために弁護士と相談して書くようなものなので、なかなか、リスクコミュニケーションの道具としては適切なものとはならない。また、事業者側の責任が限定されるようにしか書かれていないのが現実だと思う。一方で、人々が世の中にあるものを全部知り尽くして、理解して使っているかというと、そうではない場合の方が多いでしょう。恐らくは、先ほど相場観という言葉が何度か出ていたが、ＩＴの世界のリスクの多くは、どれもこれも新しくて相場観が出来ていないから起こっているということが非常に多いと思う。そこの中で、ベンダーは専門家が分かる言葉で、ある範囲で必要な情報を開示して行かなくてはならないが、リスクが分かっていれば自ら直しているという問題が殆どで、ベンダー自身も自社製品のリスクというものを正確に把握しているとは限らない。すると、問題が起こったときに誠実に対応するくらいのことしか出来ることがない。むしろ、今は技術的な問題よりも、フィッシングにしても、振り込め詐欺にしてもセキ

ュリティでは人間側の問題が増えてきていること考えたときに、もちろん事業者側が責任を持って、説明責任を果たして行くということも必要だが、それ以上に、社会としてこれを使ったらどんなことが起こるのかという、相場観を出来るだけ早く形成していって、誰にでも分かる言葉で共有されて行くような社会をしっかり造って行くということが、非常に重要だと思う。リーディングカンパニーであれば、そういった説明であるとか表示に多大なコストと専門家を投入することは出来るが、そうすると、新しい人たちが新しいことを始められない社会となるので、むしろ、問題が起こったときの説明責任をどこまで明確化するかということと、社会全体として出来るだけ早く相場観を形成し、それをブロードに広めてゆくというところの機能が非常に重要だと思う

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
将来ビジョンと技術像の検討の進め方について
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

資料に沿って説明

○　全般に付いての意見があるのですけれど、何度か行動経済学的にどうかという話があったと思うのですが、個々の議論は概ね安全のための技術がカバーされているような気がするのですが、安心のための技術というのが抜け落ちているような印象があるので、もう少しその点を埋めてゆくことが非常に重要ではないかと思う。報道の問題などもあるが、本来のリスクとそれに対する消費者の印象のギャップが非常に激しいと思う。ニュースになるものについては非常に小さなリスクであっても、安心を脅かすものとして認識されている一方で、本来もっとケアが必要となる問題について、これが社会的にクローズアップされていないとリスクが過少に見積もられていて、そこで問題が起こるというケースが増えている。よって、全般的に安心にフォーカスをした検討課題というものを入れて行くと良いのではないかと思いました。

○　例題として上げられるものはどんなものですか。

○　例でいいますと、ウィルス対策は 2003 年ころ非常にクローズアップされたのですが、最近は意識が非常に低くなっています。これは何故かというと、これまで愉快犯的だったものが、経済的利益を目的としたターゲッテットアタックの割合が非常に増

えて攻撃が見えにくくなり、本来、もっと真剣に取り組まなければならないセキュリティ対策に対する意識が非常に低くなっていると思います。一方で、先の国会で青少年ネット規制法が可決しましたが、あれなどを見ても青少年を対象とした犯罪全般は非常に減っているにもかかわらず、同じ事件が繰り返しワイドショーなどで報道されることによって、ネットが危ないというイメージを非常に強く高めたことが国会での動きに繋がったと思っています。そうした両方の意味で政策を考える上でも、本来のリスクを把握するための技術をもっと考えて行く必要があるし、特に安心という面では、安心できるようにするためには、過大にリスクが考えられているものについて大丈夫だと説明する必要があるし、むしろ問題なのは、安全ではないのに安心してしまっているところなので、注意喚起の仕方についても考えて行く必要があると思う。

○　３Ｐの社会潮流予測について、これは多分前提が各委員それぞれあると思うのですが、一つは、経済活性化の目的で将来の借金を背負うような話もあるようですが、いずれにしても今後５年１０年ということを考えると、社会コストを IT によって下げてゆくということが命題だと思う。もう一つは高齢化社会。そういったベースがあった上で、こういったものが出ているので、その辺りの各委員の想定されている５年１０年の部分も入れた方が良いかと思う。

２点目としては、７Ｐの利用者個人の部分、端末のセキュア化とか端末の安全性向上とか、不正プログラムに強い計算機、不正操作云々ということで、どちらかというと、安全の部分で全てカバーされている訳で、やはり、ナビゲーションであるとかコミュニケーションであるとか、自分の状況を教える様な部分であるとか、そちらの方を、むしろ優先しなければならないし、これは、サービスベンダーなどにも関連することだと思う。我々日本人の１つの事件も許さない、徹底的に排除して行くというような気持ちは非常に良いものだし、それ故、日本はセキュリティとか品質におけるイニシアティブというのがあるのだと思う。それ故、ガラパゴスとなるのかもしれないが。ただ、そういった観点は重要だが、やはり、知らせて行くとか、そういったことをして行かないとトータルのコストが合わない、その辺りも観点として加えてもらいたい。

○　初回の事務局の説明を思い出いだすと、今回のグランドチャレンジのＷＧはビジョナリーアプローチをしたいということだったと思います。今回７Ｐ以降にまとめられているものは技術のアイテムベースであって、最終的にビジョンとして何を実現したいのか、例えば今後ユーザーに対して、こうお願いしたいとか、あるいは攻撃側に対してあなたのところは、これから、ドンドン監視されて行くぞ、我々はドンドン情報

で優位に立って行くぞというメッセージを伝えたいのだとか、最終的に我々が何を目指したいのかと言うことが伝わりそうな書き方を加えると良いのではないかと思います。

○　資料５の方になるが、これから作ろうとしている報告書では、７－９Ｐに出ているようなマップが自然と出てくるようなストーリー、背景色の部分の話しを作文する予定をしている。各委員には将来予測について書いて頂いていますが、その辺りを取り込みながら、なめらかにシームレスに繋がるような話として作文する予定です。

○　先ほど委員が言ったのは、背景がどうなるというというより、どうするということが含まれているわけですね。

○　そうです。社会に対して伝えたいメッセージをより明確に出した方が良いと思う。

○　５Ｐとか９Ｐにクラウドとかグリッドという言葉がありますが、これは、５年とか１０年とか感覚で見た場合ユニバーサルな用語だろうか。

○　テクニカルタームとマーケティングタームということで考えると、テクニカルタームの言葉は割と定着しますが、マーケティングタームの言葉はコロコロ変わる。例えば「WEB2.0」などは正にそういう例、「クラウド」も少しマーケティングターム寄りの感じがします。

○　昔からある古い概念を新しく説明し直すときに、新しい言葉を造ったということかもしれないが、マーケティングのタームをなるべく抑えて本質的に起きる状況というのを出来るだけ的確に説明できるように wording したいと思う。

○　既に NISC の基本計画検討委員会でも議論されていることに、事故前提社会というのがあったと思います。先ほどの議論にもあったように、もし、何かあって今まで IT に頼っていたものを人がやらなくてはならないとなった時に、実は人が対応できない

状態が生ずる。そこは個別の技術アイテムではありませんし、書き方は難しいと思うのですが、この点をどう織り込んで行くかが重要だと思います。

それと、ユーザーとのリスクコミュニケーションですが、それは単純なアグリーメントの話だけではなくて、実際に新しいパラダイムというか、流れを世の中に導入したいと思っているときには、個別の製品のアグリーメントではなくて、もっと他の方法の模索が必要だと思う。例えばイギリスでは社会技術の一つとして、ベンダーや政府などが、司法でいうと陪審員に近い形でコミュニティから一般市民を選抜して、検討中の政策について意見を聞き、何度も議論するような仕組みが最近出来つつあると聞いている。公聴会でもなくパブコメでもない新しい手法を使っている訳ですが、その市民にも意識が高くてベンダーや政府にモノを言いたい人が沢山いる。そういった方々を上手く取り込んで、彼らを市民社会のユーザ側のオピニオンリーダーとして議論を広げて行く、そういう仕組みも社会技術としてはある。このようなコミュニケーションの在り方について、日本ではまだ答えがないので、アイテムベースでは書けないとは思うが、５年、１０年という先を考えると、そういった模索も必要なのだと思う。

○　技術マップの書き方で追加の提案ですが、今は、３年５年１０年という実現時期で書かれているが、それとは別にカバレッジを考えたときには、こういうリスクがあるのではないかという予期の部分、起こったことを発見する部分、起こった後に現状復帰を出来るだけ急ぐ、あるいは、後工程の原因を分析する部分などという形で、ある確率で事故が起こると分かった場合、そのリスクコミュニケーションという形で、issue ごとのライフサイクルのようなモノがあると思う。そのなかで、初めから終わりまでの技術をマッピングするということも出来るのではないかと思う。リスクコミュニケーションというのは、最後の部分、ある割合で事故が起こっている時に、それをどう周知するかと問題ですし､恐らく､これからますます不確実になってゆく中で、出来るだけ早くこういう事は起こりうるのではないかという予期をする部分と、起こったときに､それを早く発見するというところが非常に重要になってくると思います。そこは、今、非常に進歩を遂げているところでして、当社もＯＳのクラッシュダンプを利用者の任意で送ってもらう仕組みを造ることによって、Nullday アタックが起こった場合に、その日の内に把握するようなことも実際に始めていて、検知をしたときには、被害者の方々には早めにコミュニケーションを取ったり、月１回のパッチの配布のところを緊急で配布したりといったところは、瞬時に問題を理解して即応体制を執ることしていますので、事故に対するライフサイクルで技術をマッピングして行くと、抜けている部分や評価すべき部分がまた見えてくるかもしれないと思う。

○　３P でも話が出ましたけれど、２つ要素として明確に書いた方が分かり易いかなと思ったのは、「個人利用者」というレイヤーがあるのですが、あくまでもこれは個人利用者を対象としてベンダーやメーカーが考慮しなくてはならないことという観点なのです。ただ、先ほど委員からも指摘がありましたように、本当の「人」というのを上に考えたときに、その「人」から見たときに問題となるリスクコミュニケーションとか、相場観が分からないとか、「人」に依存する満たされていない要素というのがあると思う。そこを抜き出して、「人」に向けて何を手当するのかというレイヤーを設けて、やらなくてはならいことを書いた方が分かり易いかなと言う点が一つ。もう一つは脅威、悪い奴という要素を抜き出した書き方を抜き出した方が分かり易い。先ほどのミサイルの発射元という話があったが、そのとおり大事な要素であると思う。

例えばこの表の一番下に「脅威」というレイヤーを書いたとして、一番上に「個人」というレイヤーを書いたとしたら、資料に書いてある３つの色分けされたレイヤー（個人・利用者、サービス・ベンダー、社会基盤・制度）というのは、極論すれば、攻撃から消費者を守るためにやらなくてはならいことをレイヤーに分けて書いていることになると思う。一番下に脅威というものを書くことによって、先ほどのミサイルの発射元をちゃんと体系的に、組織的に追って行くという大事な技術的要素も見えてくるのではないか。見た人が分かり易いという観点から、「個人」、「脅威」の２点をはっきり書いた方が良いと思う。

○　先ほどの消費者とのコミュニケーションを日本的なアプローチでどうするかということを考えたときに、自分の行動で危険な領域に入るというのを認識させると言うことも、一つの手だと思う。例えば、携帯だと SIM というものがあって契約した情報が入っているが、これを携帯電話に差した瞬間に料金がかかるという仕組みと同じような方法で、個人認証や、ここに掲げてある技術を複合的にユーザーに理解させることができれば、行動から危険な領域、例えば、ネット家電でも買ってきて、そのまま使えてしまっては何が起きているか分からないので、何かを入れないと動かない様にするなどのことがあると思う。パソコンもネットワークに繋がった瞬間に、繋げるということを認識して、接続した瞬間に何かおきるなど、コミュニケーションだけではなく、手順や仕組み等で、上手くそういったことができると面白いと思う。

○　アクションを求める様なものでは、シールの封を切ったら同意したものと見なしますというようなものも確かにある。

○　私はそれに大賛成だ。ＰＣやネットでは自分の状態を示す指標が少なすぎる。非常に危険な操作をしているのに、それが安全なものと変わらない外観と操作で出来てしまう。それは、けしからんと思っていて、例えば銀行のサイトに行ったならば、ウィンドウの枠が真っ赤になって点滅するとか、「今から振込で良いですか？」と爆発しそうな勢いで点滅するとか、それくらいのユーザーの意識をポジショニングが分かるようにする必要がある。CCC（サイバー・クリーン・センター）などではウィルスに感染していると見つけて教えてくれるのですが、駆除したという反応がだんだん無くなってきていて、まあ、どうでも良いような人もいるのでしょうが、そのような人もパソコンの枠が真っ赤にピカピカ光っていたら、何かやらなくてはいけないのではないかと思うようになるのではなか。そういったテクノロジーでユーザーの注意喚起を、自然にやって行くという方法があっても良いのではないか。これは、グランドチャレンジではなくて、皆で合意すれば直ぐに出来ることだと思う。

○　windows vista では、例えばシステム管理者権限を持ったユーザーであっても、システム権限を要するＡＰＩ呼び出しがあった場合にブラックアウトして、「本当によろしいですか？」というダイアログが出るようになった。しかし、これが大変不評で次の windows7 では、危険な操作があった場合に過去のいくつかの履歴が簡単に辿れるような仕組みにして、逆にユーザーエクスペリエンスに関しては、XP に近いような形に戻すことになるというように試行錯誤している状況である。結局危険といっても、ソフトをインストールしても何しても同じ画面が出ると、これは行動形態学上の知見を有するでしょうが、皆慣れてしまって考えずに「Yes」を押すようになる。機械が本当にそれをリスクの高い操作なのかということを、今は、単純に API 呼び出しの権限の深さ等で判断しているが、もっと、ヒューリスティックにリスクを解析するための手法とかを研究をしなければならないし、特にそれを利用者にどう見せるかというところは、機械的な判断とは別の考えというものがもっと必要になってきていると思う。

もう一つは、銀行のサイトに行ったときに、赤い縁が出るという話なのですが、EVSSL とう仕組みで大事なサイトに関しては、グリーンの帯でそれが本物かということを見せるという技術を IE 7 から採用していますが、EVSSL の証明書売れないのでなかなか普及しないとか、反対に、今、疑わしいサイトというのを黄色で表示して、フィッシングサイトの場合には通報してもらう仕組みを導入したのですが、これが、例えば firefox 等の他のブラウザでは SSL で通信中であるという別の意味だったりして、利用者からの見え方を業界で統一して行くという、非常に難しいという現状がある。特に、銀行のサイトも銀行のドメインでやっているところばかりではなくて、例

えば、”anser.or.jp”の下に一杯並んでいるなどのこともあり、銀行によっても、そのドメインが本当に銀行のものか分からないようなドメインの取り方をしているところが多いという状況もあり、OS だけではなくて、それぞれのサイトで行動規範を合わせて行かなくては、本当に利用者からみて一貫した操作性というのは実現が出来ないが、SSL 証明書の運用一つ見ても、そこで足並みを揃えていくということは、極めて難しいというのが実感です。

○　今の意見は同感なのですが、例えば赤くすると何故赤くなったのかとか、自分はどうすれば良いのかという反応が起こる。単純にそれだけをやると、単にパニックを起こすだけになるという気がする。私は、企業の中でセキュリティの啓発活動などをする立場にあるが、その辺りが一番気を遣うところです。注意喚起を一発出すのは良いのですが下手に出した後に来る反応は、これをやってはいけないのか？どうしたらいいのかという？質問責めです。考えられるのは、一般の消費者や一般のユーザーが上手く相談できるようなところ、消費者センターさんとか、これはＩＴレベルで業界主導になるのか国が主導になるのか分かりませんが、そういう、駆け込み寺的なものが出来ないといけないと思うところ。個々のメーカーでは、テクニカルに警告を出すなどの対応はありますが、出し方によっては戸惑う場合もあるだろし、慣れてしまって意味が無くなってしまうケースもあるだろうし、その辺り等は人間系も含めて慎重に考えなくてはいけないと思う。

○　実は、どういう利用者向けの情報の出し方をすることが本当に危機を回避する上で有用であるかさえ、科学的な研究がされておらずベンダー毎に模索されている状況ですので、本当に利用者にとって便利かつ有用な注意喚起の仕方自体の模索も、非常に重要なグランドチャレンジのテーマになると思います。また、そのユーザービリティテストの手法等（たとえば、標準化、方法論など）が確立できれば、セキュリティ全体の底上げになると思いますので、それ自体グランドチャレンジの素晴らしいテーマだと思います。

○　そのような分野は、日本の賢い消費者の目といったもので、他の国からは、日本が率先してそういう取り組みをして確立して欲しいと思っているかもしれない。

○　そういったものは、これから出てくるネット家電などに最初から入れて行けば、Ｐ

Ｃで起こったことが起こらない可能性が高くなると思う。

○　確かに、これらは個別にやっていても仕方がないので、優れたものがあればそれを共有するとか、誰かが号令掛けるとか、上手いやり方をするとか、教育であるとか、複合的にやらなくてはならいところだと思う。ご指摘のように、技術の専門家だけでも解決しないところがあるが、そういったところを研究されている方も世の中にはいるので、充分連携を取って進める必要があるかなと思う。

○　今は、こういうことを政府広報することは無いだろうが、５年１０年後はするかもしれない。そのようなときのコミュニケーションの仕方や何かあったときに、国民に知らせる手段などは考慮しておいて良いかなと思う。

○　緊急の避難情報とか警告とかを自治体でどのように集約して行くか議論しているところがありますが、そこでの話だと、今はあまり集約されていなくて、報道機関とか行政機関とか重要インフラの方がファクシミリを飛ばして発信している現状があって、受ける方は情報が膨大な量になっている。そして、その情報がどれくらい信頼性のあるものであるとか、その情報を編集して良いのかなど様々な問題があるようです。そういう状況だと、情報を出す人が必死に緊急の情報だと言って送っても、見る方がそう情報を見なければ何にもならないという指摘もあるようです。だんだん世の中に、情報を使いこなすことが人間の基本的な権利だという感覚も出てきていますので、それが先ほどの発言があったように、自分の情報なのに自分で使いこなせないということになれば、非常に大きい社会的損失ですから、そういったところも含めて考えて行く必要があるかと思います。

＊＊
報告書２次案について
＊＊

○　資料に沿って説明

○　なお、先ほどの議論の中で指摘のあった、ビジョンの部分については、明確に書かれていないので、５章の中にいれるか新しく項を立てるかは分かりませんが、考えて行きたい。

○　先ほどの議論のあった部分は、補って行くと言うことで事務局から説明がありました。

○　ビジョンというものは、できるだけ誰にでも分かるシンプルな一言二言の言葉で大きく頭に欲しい。先ほどの委員の話にもありましたが、こうしたいという意志を感じるものにしたいと思う。何となく、先ほどの将来予測の話でもそうですが、今は、遠巻きに将来はこうなってゆくと議論しているのですが、それを集めても、ちょっと発散する感じがある。我々の国はこうしたいということがあって、そこから、落として行くというのがあると、良いのではないかと思う。

○　なるべく強めのメッセージ性を伴って、こうあるべしと言うようなことを書きたいと思う。

○　ただ、気になるのは、具体的にどう書くかというところ。ＩＴがいろいろ進んでモニタリングされて、プライバシーも脅かされるおそれがあるし、非常に安全だけど自由はつらつとしたところがない世界になると書くか、そうではなくて、自由活発なことが出来るのだけれど、リスクも自分で負わなければならない世界になると書くか、かなりスパンが広いので、それを言うのはかなり難しい。そういう場合で普通するのは、あまり明確に書くのではなく、両論を併記する書き方になるような気がする。

○　今後を考えると、ネットヘブンのようなこともある。例えば日本がネットヘブンということになれば諸外国からも含めて沢山商売をしに日本にやってくる。逆もまた真なので、例えば別の国がネットヘブンになると、そこから日本向けにサービスをしませんかとなる。クラウドの中の経済戦争で、どう日本はやって行くのかという観点も必要。

○　多分多くのセキュリティ・プライバシーの問題は、突き詰めていくと、ＩＴが当たり前の社会になったのに、ＩＴの振る舞いというのが当たり前とか常識から外れたことが沢山あるということが根にある問題という気がする。それを解決するためには、

普通の人の直感に反さない社会インフラに、如何にＩＴをしてゆくかということが重要で、自己責任・リスクテイカーの場合も、自分はリスクを取っているのだから当たり前だと思うのであり、あまり深く考えないでいろいろなものの恩恵にあずかっている人も､世の中こう当たり前だなと思うような相場観を創るということもそうですが、世の中の相場観にＩＴが合わせて行かなくてはならないという点がとても重要で、そういうことを上手く言える言葉がないかなと考えました。

○　メッセージとしては、両論併記でプレーンに書くよりも、未来を明るく見た上で、しかし、セキュリティとしてここはこのようにしっかりやっていく、という、割り切ったビジョンが良いかと思う。なおかつ、ユーザーとのコミュニケーションでもそうだが、悪者に対して懲らしめるようなメッセージを与える必要がある。また、情報セキュリティの業務は日が当たらないので、これから細って行くおそれがあると聞いている。これは、若い優秀な人が情報セキュリティの業界に集まってこないということにも繋がっているので、学生やセキュリティを目指している人に対しても、やり甲斐とかモチベーションを与えるようなメッセージを含んだものを書く必要があるだろう。それは、この全体の目次の中では、どこかに入れづらいかもしれないので、全体のサマリーとして持ってきて、その中にメッセージを書く方法もあるかもしれない。その辺りも考えて進めて欲しい。

○　各委員もそれぞれの分野でこのようなものを作る立場にある方だと思いますし、先程から出ているとおり、主体的にこれからどうするというような考えをお持ちの方が多いので、書き方、どうすれば説得力がでるのかという点を指摘していただき、ありがとうございます。

私も、脳の研究をやっている方と話をすると、そうそう、人間というのは変わっているわけではないのだと。一見、新しいことが出来るように見えるのだけれど、なかなか限界もあるのだから、そこを充分考えないと失速するというか、使いこなせないものが出来てしまい、結局皆が困ることになるかもしれないと指摘がありました。

以上